

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA**

Alexandria Division

UNITED STATES OF AMERICA,)	
)	
v.)	
)	Case No. 17-cr-135
BRIAN HONIG LEONARD,)	Hon. Liam O'Grady
)	
<i>Defendant.</i>)	
)	

MEMORANDUM OPINION & ORDER

Pending before the Court are Defendant Brian Honig Leonard's Motion to Suppress Network Investigative Technique ("NIT") Search and for a *Franks* Hearing (Dkt. No. 37) and Motion to Suppress Home Search (Dkt. No. 39). For the reasons described below, the Court hereby **DENIES** both motions.

I. Factual Background

The Defendant was charged with Receipt of Child Pornography in violation of 18 U.S.C. § 2252(a)(2) and Possession of Child Pornography in violation of 18 U.S.C. 2252(a)(4)(B) following an investigation into a website called "Playpen," which the government asserts operated as a child pornography site. *See* Indictment, Dkt. No. 20. The Playpen site operated on what is known as the "Tor" network, which enables its users to conceal their Internet Protocol ("IP") addresses after they download a browser from the Tor website. *See United States v. McLamb*, 220 F. Supp. 3d 663, 666 (E.D. Va. 2016). User communications on the Tor network are transmitted to various points among a network of computers before reaching the destination computer, which makes it difficult to discover users' identifying information, including their IP addresses. *Id.* at 667. Tor network users can use Tor indices to locate hidden sites, which could

not be located on typical Internet search engines. *Id.* Because these sites are hidden, a user of the Tor network cannot simply run a search to find a site of interest to the user. *See United States v. Euse, 2:16cr43, 2016 WL 4059663 at *2 (E.D. Va. July 28, 2016)* (“[A] user cannot simply stumble onto a hidden service”). Instead, the user must obtain the address in advance, through postings on the Internet or by communications with other users of the Tor network. *Id.*

Therefore, to access the Playpen site, a user had to either know the specific site URL or locate Playpen via the Tor index. *McLamb, 220 F. Supp. 3d at 671.* Once at the site, the user would have had to go to the homepage, click past the warning that only members were permitted, create a username, and register an account. *Id.* At the registration stage, potential users were warned not to enter a real email address or post identifying information in their profiles. *See NIT Affidavit, Dkt. No. 38-1 at 14.* There were thus several affirmative steps that a user would have to have taken to access the Playpen site, and it stands to reason that an accidental visitor would not have completed the steps without having any idea as to the site’s content. *See McLamb, 220 F. Supp. 3d at 671.*

Despite the anonymity offered by the Tor network, the government is able to recover identifying information of Tor users through a Network Investigative Technique (“NIT”) search. *See Government’s Opposition to Defendant’s Motion to Suppress NIT Search, Dkt. No. 41 at 1-2.* The NIT was a piece of computer code that, once downloaded to a computer, would search that computer for certain identifying information. *Id.* In this case, the NIT search operated as follows: the FBI seized control of Playpen’s server, and added the computer code comprising the NIT to the digital content of the Playpen website. *Id. at 6.* From that point, when a computer user logged into the Playpen site with a username and password, an application instructed the user’s computer to send identifying information to a different, government-controlled computer.

Id. at 6-7. The NIT extracted from the user's computer (1) the IP address of the computer and the date and time this information was determined; (2) a unique identifier that would distinguish the user's computer's data from other computer's data; (3) the type of operating system used by the computer; (4) information about whether the NIT had already been sent to the computer; (5) the computer's "Host Name," which is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, including communications over the Internet; (6) the computer's operating system user name; and (7) the computer's media access control ("MAC") address. *See* NIT Affidavit, Dkt. No. 38-1 at 25-26; *see also* *Eure*, 2016 WL 4059663 at *3.

The initial NIT search of Defendant's computer occurred between February 20, 2015 and March 4, 2015. *See* Defendant's Memorandum in Support of Motion to Suppress Home Search, Dkt. No. 40 at 1. On July 27, 2015, the FBI applied for a search warrant for Defendant's home based on information elicited via the NIT search. *Id.* Both the affidavit in support of the NIT warrant and the affidavit in support of the home search warrant contained what the Defendant describes as a "false and misleading" description of the image appearing on the Playpen homepage. Defendant's Memorandum in Support of Motion to Suppress Home Search, Dkt. No. 40 at 2; Defendant's Memorandum in Support of Motion to Suppress NIT Search, Dkt. No. 38 at 4. Defendant seeks to suppress the NIT search of his computer on various grounds. He argues that a *Franks* hearing is necessary due to the affidavit's inaccurate description of the images on the Playpen homepage, that the NIT warrant violated the Fourth Amendment probable cause and particularity requirements, and that the NIT warrant was issued in violation of Federal Rule of Criminal Procedure 41(b). He also seeks the suppression of the home search on the grounds that

the probable cause information contained in the supporting affidavit was stale, limited in duration, and insufficiently corroborated.

II. A *Franks* Hearing is Unnecessary

A *Franks* hearing is warranted where (1) the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit; and (2) the allegedly false statement is necessary to the finding of probable cause. *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978).

Defendant claims that the NIT search warrant application contained a “clear falsehood” that was central to Magistrate Judge Buchanan’s probable cause determination. *See* Defendant’s Memorandum in Support of Motion to Suppress NIT Search, Dkt. No. 38 at 5. Specifically, the application incorrectly described the image that appeared on the front page of the Playpen website. *Id.* at 4. The application described the homepage as containing “images depicting partially clothed prepubescent females with their legs spread apart.” NIT Affidavit, Dkt. No. 38-1 at 13. However, at the time the warrant was signed, the homepage displayed a different image. It showed a prepubescent girl, wearing a short dress and black stockings, reclined on a chair with her legs crossed and posed in a sexually suggestive manner. Government’s Opposition to Defendant’s Motion to Suppress NIT Search, Dkt. No. 41 at 8. The Government has explained that the description of the image on the Playpen homepage in the NIT search warrant application was inaccurate because the Playpen site administrator changed the image sometime between February 18, 2015, when the affiant last reviewed the Playpen site, and February 20, 2015, when the affiant swore to the NIT warrant. *Id.* The affidavit did not reference the change in images because the Government was not yet aware of the logo change. *Id.* The Court finds that the Government’s explanation for the affidavit’s inaccurate description of the Playpen homepage is

reasonable, and that Defendant has made no showing that the description of the Playpen homepage made in the affidavit was knowingly or intentionally false, or made with reckless disregard for the truth.

III. Probable Cause Existed for the NIT Warrant, and the Warrant did not Violate the Fourth Amendment's Particularity Requirement

A court reviewing whether a magistrate judge correctly determined that probable cause exists should afford the magistrate judge's determination of probable cause great deference. *United States v. Matish*, 193 F. Supp. 3d 585, 602 (E.D. Va. 2016) (citing *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). The duty of a reviewing court is simply to ensure that the magistrate judge had a substantial basis for concluding that probable cause existed. *Id.* Defendant asserts that the magistrate judge's judgment had no "substantial basis" for her finding of probable cause, because the "mere act" of logging onto the site was insufficient to create probable cause that contraband or evidence of a crime would be found on the user's computer. *See* Defendant's Memorandum in Support of Motion to Suppress NIT Search, Dkt. No. 38 at 16. As described above, users had to take multiple affirmative steps to log in to the Playpen website, and it is unlikely a user could do so without knowledge that the site was dedicated to child pornography. *See United States v. Darby*, 190 F. Supp. 3d 520, 532 (E.D. Va. 2016) ("Defendant fails to explain why someone would go to the trouble of entering the Tor network, locating Playpen, registering for the site, and then logging into the site if they were not looking for illegal content. It is not as if the Internet is not saturated in legal pornography. The magistrate judge's common sense judgment would justify her finding that an individual would likely only take these steps if he was seeking child pornography and knew he could find it on Playpen.").

The fact that the affidavit did not accurately describe the exact image that appeared on the Playpen website at the time the warrant was issued does not change this analysis. It is

irrelevant that the old image on the Playpen homepage was *more* indicative of child pornography than the image actually in place at the time the affidavit was sworn. *See Darby*, 190 F. Supp. 3d at 531 (“To the extent one can or should differentiate among sexualized depictions of children, the images of the two girls that were previously on the homepage are more reprehensible. But that distinction does not subtract from the sexualized nature of the single image of child erotica that appeared on the homepage . . .”). Courts in the Eastern District of Virginia have already ruled that this image change was not material to the probable cause determination, and this Court finds no reason to depart from those rulings. *See, e.g., United States v. McLamb*, 220 F. Supp. 3d 663 (E.D. Va. 2016); *United States v. Matish*, 193 F. Supp. 3d 585 (E.D. Va. 2016); *United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016). Additionally, the abundance of other evidence before the magistrate judge supported her finding of probable cause. *See* Dkt. 41 at 13.

Defendant additionally argues that the NIT warrant was unconstitutionally overbroad and violated the particularity requirement of the Fourth Amendment because the warrant identified the place to be searched as the “activating computers,” which were those computers of a user who logged into the Playpen website by entering a username and password. *See* Defendant’s Memorandum in Support of Motion to Suppress NIT Search, Dkt. No. 38 at 19. The Fourth Amendment requires that search warrants “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV. This particularity requirement mandates that a warrant “be no broader than the probable cause on which it is based.” *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006).

Here, the scope of the NIT warrant was tailored to the probable cause that supported it. The probable cause supporting the NIT warrant was based on the likelihood that any given Playpen member possessed child pornography, or evidence of related crimes, on the computer

from which he accessed Playpen. Government’s Opposition to Defendant’s Motion to Suppress NIT Search, Dkt. No. 41 at 23. Given that theory of probable cause, the natural scope of the NIT warrant was to search any computers that were used to access Playpen. *Id.* Every court to consider this question has found the NIT search warrant sufficiently particular, and this Court sees no reason to differ. *See United States v. Anzalone*, 208 F. Supp. 3d 358, 368 (D. Mass. 2016).

IV. The Magistrate Judge had Authority to Issue the Search Warrant under Rule 41

Federal Rule of Criminal Procedure 41(b) instructs that “a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district.” Fed. R. Crim. P. 41(b)(1). The search challenged here was of the Defendant’s computer in Woodbridge, Virginia, which is located within this district. Therefore the NIT warrant was a proper exercise of the magistrate judge’s authority. *See United States v. Workman*, 863 F.3d 1313, 1319 n.1 (10th Cir. 2017); *Anzalone*, 208 F. Supp. 3d at 372 (“Even if the magistrate judge in the Eastern District of Virginia lacked the authority to issue a warrant that allowed the FBI to deploy the NIT outside of that district, the magistrate judge did have authority to issue a warrant in which the NIT deployed in that district.”).

Rule 41(b)(4) further authorizes a magistrate judge “to issue a warrant to install within the district a tracking device,” and the warrant “may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both.” Fed. R. Crim. P. 41(b)(4). This Court finds that the magistrate judge had authority to authorize the NIT search warrant even though the tracking capabilities could ultimately impact out-of-district computers. *See McLamb*, 220 F. Supp. 3d at 673 (explaining that so long as the tracking devices are installed within the district, they can permissibly operate even after the device leaves the

district where it was installed, and finding the NIT search warrant analogous); *Matish*, 193 F. Supp. 3d at 613 (“[W]hen users entered Playpen, they came into Virginia in an electronic manner . . . When that computer left Virginia—when the user logged out of Playpen—the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target’s location.”).

Even if the warrant had been issued in violation of Rule 41, this Court finds that the good-faith exception to the exclusionary rule applies here. *See United States v. Leon*, 468 U.S. 897 (1984) (holding that when police act in “objectively reasonable reliance on a subsequently invalidated search warrant” obtained from a neutral and detached magistrate, “the marginal or nonexistent benefits produced by suppressing evidence” cannot justify the costs of exclusion); *Herring v. United States*, 555 U.S. 135, 141 (2009) (holding that suppression of evidence is appropriate only where police conduct is sufficiently deliberate that the exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system); *United States v. Doyle*, 650 F. Supp. 3d 460, 467 (4th Cir. 2011). Courts in the Eastern District of Virginia have similarly ruled that the agents in the Playpen investigation could reasonably rely on the magistrate judge’s determination that she had authority to issue the warrant. *See Eure*, 2016 WL 4059663 at *9 (“It was quite logical for the FBI agents to seek this warrant in the Eastern District of Virginia. Because the FBI planned to run the website from a server located in the district there was no district in the country that had a stronger connection to the proposed search.”).

V. The Search Warrant on Defendant’s House was Appropriate

The exclusionary rule provides that evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of an illegal search and

seizure. *See United States v. Calandra*, 414 U.S. 338, 347 (1974). The Supreme Court established an exception to the exclusionary rule in *Leon*, finding that “suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual circumstances in which the exclusion will further the purposes of the exclusionary rule.” *United States v. DeQuasie*, 373 F.3d 509, 519 (4th Cir. 2004) (citing *Leon*, 468 U.S. at 918).

There are four circumstances in which the *Leon* good faith exception would not apply: (1) if the magistrate judge in issuing the warrant was misled by information in an affidavit that the affiant knew was false or would have known was false but for his reckless disregard of the truth; (2) if the issuing magistrate judge wholly abandoned his or her judicial role; (3) if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the warrant is so facially deficient that the executing officers cannot reasonably presume it to be valid. *See DeQuasie*, 373 F.3d at 519-20 (citing *Leon*, 468 U.S. at 923) (internal punctuation omitted).

Here, Defendant argues that the affidavit supporting the home warrant lacked sufficient information to support the magistrate judge’s finding of probable cause. *See* Defendant’s Memorandum in Support of Motion to Suppress Home Search, Dkt. No. 40 at 3, 9.

But Defendant has failed to show that the probable cause supporting the home search warrant was so lacking as to render reliance on it unreasonable. First, there was sufficient information for Magistrate Judge Davis to determine that the Defendant intentionally accessed the Playpen website for the purpose of viewing child pornography. *See* Government’s Opposition to Defendant’s Motion to Suppress Home Search, Dkt. No. 42 at 3 (explaining that the affidavit described the “numerous affirmative steps” Defendant must have taken to access the Playpen website, showed that Defendant “accessed three posts containing extremely graphic and

obvious child pornography,” and demonstrated that the IP address used to access those posts traced back to the Defendant’s home address).


Second, Defendant’s staleness argument is unavailing. Because the affidavit stated only that Defendant was logged into the website for a total of 1 hour and 26 minutes between February 18 and February 27, 2015, Defendant argues that there was no probable cause to believe that child pornography would be found at his home on July 30, 2015. *See* Defendant’s Memorandum in Support of Motion to Suppress Home Search, Dkt. No. 40 at 3-4. But the question of staleness is determined by all the facts and circumstances of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized. *See United States v. Richardson*, 607 F.3d 357, 370 (4th Cir. 2010). Child pornography cases present a unique context because child pornography collectors typically store their sexually explicit material for long periods. *See id.* Courts have accepted even substantial delays between distribution and the issuance of a search warrant in such cases. *See id.*; *United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005) (“Information a year old is not necessarily stale as a matter of law, especially where child pornography is concerned.”); *United States v. Harvey*, 2 F.3d 1318, 1323 (3rd Cir. 1993) (holding that information supporting a warrant application was not stale even when several pornographic mailings occurred thirteen to fifteen months prior to the issuance of the warrant and noting that “pedophiles rarely, if ever, dispose of sexually explicit material.”). The circumstances of this case therefore justified the magistrate judge’s conclusion that the affidavit created probable cause for the home search warrant.

VI. Conclusion

For the reasons described above, this Court **DENIES** Defendant's Motion to Suppress NIT Search and for a *Franks* Hearing (Dkt. No. 37) and Motion to Suppress Home Search (Dkt. No. 39).

It is **SO ORDERED**.

October 6, 2017
Alexandria, Virginia



Liam O'Grady
United States District Judge